CS458 ASSIGNMENT 3

Ching Chuen Chia

STUDENT NUMBER: 20755359 WATID:CCCHIA

1.

a. Mallory will be able to learn alice's login information. First because he had implanted his fake root CA verification key in alice's computer, the browser will identify the phishing website as an authentic website signed by a root CA. unless Alice is very careful and always check the TLS verification and their verification keys, Mallory's attack will succeed.

b. this approach will not work as the phishing website will have different domain name from the certificate, causing the browser to identify an error and will close the site.

c. this approach will not work as the browser will see the website as the company's domain name and website, this will cause the browser to think it is the authentic company site as the website displayed will be verified by a authenticate root CA verification key in the browser and the domain is the same as the one displayed in the certificate. However, the decryption of the TLS key exchange protocol will fail and thus Mallory will be unable

d. if Mallory can find the private key in the TLS MITM program that generates the certificate for the visited site, he will be to read all traffic going through the network including alice's, as every laptop is using the same keypair.

e. Mallory is going to need access to alice's laptop to get the private key of the TLS MITM program as it generated a new keypair different from the other laptop.

2.

d. the important of fingerprint is to check the validity of the public key. If the fingerprint is not checked, attackers are able to forge fake keypair and release the key as another person and if a friend didn't check the fingerprint before certifying it, it will be valid to others.

3.

a.

Tracker = select SUM(grade) from student where Gender="M"

select SUM(grade) from student where Gender ='M' or Name = 'Blair'

select SUM(grade) from student where Gender !='M' or Name = 'blair'

select SUM(grade) from student

b.

No it is not.

Name	BirthDate	Gender	Postal Code
*	0***	M	N8M 5Q1
	1***	M	N8M 5Q1
	0***	F	V3B 9C7
	0***	M	N8M 5Q1
	0***	F	V3B 9C7
	0***	M	N8M 5Q1
	1***	M	V3B 9C7
	1***	M	V3B 9C7
	0***	F	K0L 6B3
	0***	F	K0L 6B3

L-diversity = 1